

What is claimed is:

1 1. An encrypted-data decrypting apparatus that decrypts, for  
2 a purpose of execution on a computer system, a program that has  
3 been encrypted and stored, the encrypted-data decrypting  
4 apparatus comprising:  
5 a storing unit operable to store therein the program as  
6 a plurality of partial programs having been encrypted;  
7 a memory location information generating unit operable  
8 to generate, for each of the partial programs, memory location  
9 information including (i) timing information indicating a timing  
10 of decryption and (ii) positional information indicating into  
11 which location area each partial program is to be located after  
12 being decrypted, the location area being included in a memory  
13 space used for the execution of the program;  
14 a decrypting unit operable to sequentially read, from the  
15 storing unit, and decrypt the partial programs according to the  
16 timing information; and  
17 a loading unit operable to locate each of the decrypted  
18 partial programs into each location area indicated by the  
19 positional information.

1 2. The encrypted-data decrypting apparatus of Claim 1,  
2 wherein

3           the positional information indicates, with respect to each  
4   of at least one of the partial programs, that one partial program  
5   gets overwritten into a location area where one or more other  
6   partial programs have already been located before the one partial  
7   program gets decrypted.

1   3.     The encrypted-data decrypting apparatus of Claim 1,  
2   wherein

3           the positional information is stored after being encrypted,  
4   and

5           the loading unit decrypts the positional information so  
6   that each of the decrypted partial programs gets located into  
7   each location area according to the decrypted positional  
8   information.

1   4.     The encrypted-data decrypting apparatus of Claim 2,  
2   wherein

3           at a time of locating each partial program into a location  
4   area, when a size of the location area is larger than a size  
5   of the partial program, the loading unit writes dummy data into  
6   a space area, which is a portion of the location area that has  
7   not been overwritten because of a difference between the sizes.

1   5.     The encrypted-data decrypting apparatus of Claim 1,

2 wherein

3       when a predetermined length of time elapses after one  
4 partial program located into a location area finishes being  
5 executed before another partial program gets located into the  
6 location area, the loading unit deletes the one partial program.

1 6.     The encrypted-data decrypting apparatus of Claim 1,  
2 further comprising

3       a key embedding unit operable to embed into at least one  
4 of the partial programs, in advance during a process of program  
5 encryption, part or all of an encryption key used in a decryption  
6 process of another partial program, wherein

7       the decrypting unit performs the decryption process of  
8 this other partial program, using the encryption key embedded  
9 in the at least one partial program that has already been decrypted  
10 and located in the memory space.

1 7.     The encrypted-data decrypting apparatus of Claim 1,  
2 further comprising

3       a program embedding unit operable to embed into at least  
4 one of the partial programs, in advance during a process of program  
5 encryption, an encryption key generating program for generating  
6 part or all of an encryption key used in a decryption process  
7 of another partial program, wherein

. .

8           the decrypting unit performs the decryption process of  
9   this other partial program, using the encryption key generated  
10   through execution of the encryption key generating program  
11   embedded in the at least one partial program that has already  
12   been decrypted and located in the memory space.

1   8.    The encrypted-data decrypting apparatus of Claim 1,  
2   further comprising  
3        an encryption-key-for-a-key embedding unit operable to  
4   embed into at least one of the partial programs, in advance during  
5   a process of program encryption, an encryption-key-for-a-key  
6   that is used to decrypt an encryption key which is to be used  
7   in a decryption process of another partial program, wherein  
8        the decrypting unit performs the decryption process of  
9   this other partial program, using the encryption key decrypted  
10   with the encryption-key-for-a-key obtained from the at least  
11   one partial program that has already been decrypted and located  
12   in the memory space.

1   9.    The encrypted-data decrypting apparatus of Claim 1,  
2   wherein  
3        the loading unit dynamically determines an absolute  
4   address of each location area before one of the partial programs  
5   that is to be decrypted first gets located into the memory space.

. .

1 10. The encrypted-data decrypting apparatus of Claim 1,  
2 wherein  
3 the decrypting unit decrypts each partial program with  
4 use of a decryption support program,  
5 the encrypted-data decrypting apparatus further  
6 comprises a decryption program confirming unit operable to  
7 confirm authenticity of the decryption support program, and  
8 the decrypting unit has the decryption program confirming  
9 unit confirm the authenticity of the decryption support program  
10 before decrypting each partial program, and decrypts each partial  
11 program only after the authenticity is confirmed.

1 11. The encrypted-data decrypting apparatus of Claim 1,  
2 further comprising  
3 an illegitimate access preventing unit operable to, when  
4 detecting an interruption, perform an illegitimate access  
5 preventing process by deleting one or more partial programs that  
6 are already located in the memory space.

1 12. The encrypted-data decrypting apparatus of Claim 11,  
2 wherein  
3 the illegitimate access preventing unit has a dummy program  
4 executed when performing the illegitimate access preventing  
5 process.

. .

1 13. The encrypted-data decrypting apparatus of Claim 11,  
2 wherein  
3 the illegitimate access preventing unit receives in  
4 advance a registration of one or more positions at each of which  
5 an interruption for legitimate program checking occurs, and does  
6 not perform the illegitimate access preventing process when the  
7 detected interruption has occurred at one of the registered  
8 positions.

1 14. The encrypted-data decrypting apparatus of Claim 1,  
2 further comprising  
3 a storing position information storing unit operable to  
4 store therein storing position information that has been  
5 encrypted and indicates, for each of the partial programs, a  
6 storing position in the storing unit, wherein  
7 the decrypting unit reads, from the storing unit, and  
8 decrypts each of the partial programs according to the storing  
9 position information which the decrypting unit has read from  
10 the storing position information storing unit and decrypted.

1 15. The encrypted-data decrypting apparatus of Claim 14,  
2 further comprising  
3 a storing position information authenticating unit  
4 operable to judge if the storing position information is

5 authentic, wherein

6 when the storing position information authenticating unit  
7 judges affirmatively, the decrypting unit reads, from the storing  
8 unit, and decrypts each of the partial programs.

1 16. An encrypted-data decrypting apparatus that decrypts, for  
2 a purpose of execution on a computer system, a program that has  
3 been encrypted and stored, the encrypted-data decrypting  
4 apparatus comprising:

5 a storing unit operable to store therein the program as  
6 a plurality of partial programs having been encrypted;

7 a decrypting unit operable to read one of the partial  
8 programs being an execution target from the storing unit and  
9 decrypt the read partial program;

10 a memory location determining unit operable to dynamically  
11 determine a location position of the partial program being the  
12 execution target, the location position indicating an address  
13 in a memory space used for the execution of the program; and

14 a loading unit operable to locate the decrypted partial  
15 program into the location position determined by the memory  
16 location determining unit.

1 17. The encrypted-data decrypting apparatus of Claim 16,  
2 wherein

3           thememorylocationdeterminingunitdeterminesalocation  
4   positionfor each of atleast one of the partial programs, so  
5   that one partial program gets overwritten into an area that is  
6   included in the memory space and where one or more other partial  
7   programs have already been located.

1   18.   The encrypted-data decrypting apparatus of Claim 16,  
2   further comprising  
3           an execution-purpose memory determining unit operable to  
4   dynamicallydetermine, beforetheexecutionoftheprogramstarts,  
5   one or both of a start address and a size of the memory space.

1   19.   The encrypted-data decrypting apparatus of the Claim 16,  
2   wherein  
3           when the memory location determining unit determines a  
4   locationpositionofapartialprogramsothatthepartialprogram  
5   gets overwritten into an area where one or more other partial  
6   programs have already been located, the location position is  
7   determined so that the partial program overwrites such a partial  
8   program that has been located into the memory space earliest.

1   20.   The encrypted-data decrypting apparatus of Claim 16,  
2   wherein  
3           when the memory location determining unit determines a



location position of a partial program so that the partial program gets overwritten into an area where one or more other partial programs have already been located, the location position is determined so that the partial program partially or completely extends over two or more other partial programs that have been located.

21. An encrypted-program generating apparatus that encrypts a program that is to be executed on a computer system, the encrypted-program generating apparatus comprising:

a memory location information generating unit operable to generate, in order to locate the program into a memory space for the execution of the program in units of a plurality of partial programs, memory location information for each of the partial programs, the memory location information including (i) timing information indicating a timing of decryption and (ii) positional information indicating into which location area each partial program is to be located after being decrypted, the location area being included in the memory space; and

a program encrypting unit operable to encrypt the program in units of the plurality of partial programs, wherein

the memory location information generating unit determines contents of the memory location information while giving priority to confidentiality so that, with regard to each

18 of at least one of the partial programs, one partial program  
19 gets overwritten into a location area where one or more other  
20 partial programs have been located before the one partial program  
21 gets decrypted.

1 22. The encrypted-program generating apparatus of Claim 21,  
2 wherein  
3 before the partial programs are encrypted, the program  
4 encrypting unit embeds, into each of at least one of the partial  
5 programs, either (a) an encryption key used in a decryption  
6 process of another partial program or (b) data required for  
7 obtaining the encryption key, and  
8 when this other partial program needs to be decrypted,  
9 either the encryption key or the encryption key obtained with  
10 use of the data is used, the encryption key or the data being  
11 obtained from the partial program that has previously been  
12 decrypted.

1 23. An encrypted-data decrypting method for decrypting, for  
2 a purpose of execution on a computer system, a program that has  
3 been encrypted and stored, the encrypted-data decrypting method  
4 comprising:  
5 a storing step of storing, into a storage device, the  
6 program as a plurality of partial programs having been encrypted;

7           a memory location information generating step of  
8     generating, for each of the partial programs, memory location  
9     information including (i) timing information indicating a timing  
10    of decryption and (ii) positional information indicating into  
11    which location area each partial program is to be located after  
12    being decrypted, the location area being included in a memory  
13    space used for the execution of the program;  
14           a decrypting step of reading, from the storage device,  
15    one of the partial programs being an encryption target, and  
16    decrypts the read partial program according to the timing  
17    information; and  
18           a loading step of locating the decrypted partial program  
19    into the location area indicated by the positional information.

1   24.    An encrypted-data decrypting method for decrypting, for  
2    a purpose of execution on a computer system, a program that has  
3    been encrypted and stored, the encrypted-data decrypting method  
4    comprising:

5           a decrypting step of reading, from a storing unit that  
6    stores therein the program as a plurality of partial programs  
7    having been encrypted, one of the partial programs being an  
8    execution target and decrypts the read partial program;  
9           a memory location determining step of dynamically  
10   determining a location position of the partial program being

the execution target, the location position indicating an address in a memory space used for the execution of the program; and a loading step of locating the decrypted partial program into the location position determined in the memory location determining step.

25. A program that makes a computer operate as an encrypted-data decrypting apparatus that decrypts, for a purpose of execution on a computer system, a program that has been encrypted and stored, the encrypted-data decrypting apparatus comprising:

a storing unit operable to store therein the program as a plurality of partial programs having encrypted;

a memory location information generating unit operable to generate, for each of the partial programs, memory location information including (i) timing information indicating a timing of decryption and (ii) positional information indicating into which location area each partial program is to be located after being decrypted, the location area being included in a memory space used for the execution of the program;

a decrypting unit operable to sequentially read, from the storing unit, and decrypt the partial programs according to the timing information; and

a loading unit operable to locate each of the decrypted

19 partial programs into each location area indicated by the  
20 positional information.